# VERFAHREN UND EINRICHTUNG ZUM BILDEN UND ENTSCHLÜSSELN EINER VERSCHLÜSSELTEN NACHRICHT MIT KOMMUNIKATIONS-KONFIGURATIONSDATEN

Beschreibung

Verfahren und Einrichtung zum Bilden einer verschlüsselten Nachricht und Verfahren und Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht

Die Erfindung betrifft ein Verfahren und eine Einrichtung zum Bilden einer verschlüsselten Nachricht sowie ein Verfahren und eine Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht.

Ein Mobilfunk-Kommunikationsendgerät erhält im Rahmen des Netzzugangs von dem Kommunikationsnetzwerk üblicherweise eine Reihe von Konfigurationsparametern, welche beispielsweise Kommunikationsverbindungs-Parameter enthalten. Der im Rahmen der Bereitstellung der Konfigurationsparameter verwendete Mechanismus ist abhängig von dem jeweiligen Anwendungsszenario.

Für ein Mobilfunk-Kommunikationsendgerät, das sich in einem lokalen Netzwerk, beispielsweise einem **W**ireless **L**ocal **A**rea **N**etwork (WLAN) anmeldet, beispielsweise bei einem so genannten Hotspot als Zugangsknoten zu dem lokalen Netzwerk besteht die Möglichkeit der Bereitstellung von Konfigurationsparametern derzeit oftmals nicht, da weder das **P**oint-to-**P**oint **P**rotokoll (PPP) noch virtuelle private Kommunikationsnetzwerke (**V**irtual **P**rivate **N**etwork, VPN) eingesetzt werden. Erfolgt kein Schutz der von dem jeweiligen Mobilfunk-Kommunikationsendgerät verwendeten Konfigurationsdaten, d.h. der Konfigurationsparameter, so besteht für einen Angreifer die Möglichkeit, sowohl dem Mobilfunk-Kommunikationsendgerät als auch dem Kommunikationsnetzwerk Schaden zuzufügen. Eine Beschreibung der existierenden Sicherheitsbedrohungen ist beispielsweise in [1] zu finden.

**Fig.1** zeigt ein Blockdiagramm, welches eine Kommunikationsanordnung 100 darstellt. Die Kommunikationsanordnung 100 weist ein Zugangsnetzwerk 101 sowie eine Netzwerk-Domäne 102 auf, welche miteinander mittels eines Zugangs-Routers 105 (Access Router) gekoppelt sind.

In dem Zugangsnetzwerk 101 sind ferner mindestens ein Mobilfunk-Kommunikationsendgerät 103 sowie ein Vermittlungsknoten 104 (Link Node) vorgesehen, um eine Mobilfunk-Kommunikationsverbindung zwischen dem Mobilfunk-Kommunikationsendgerät 103 und der Netzwerk-Domäne 102 und darüber mit anderen Kommunikationsendgeräten, bereitzustellen.

In Fig.1 sind ferner eine Vielzahl von erforderlichen Kommunikationsprotokollen dargestellt, die im Rahmen einer Kommunikationsnetzwerk-Zugangsprozedur ausgeführt werden. Mittels der Pfeile bzw. der Doppelpfeile ist jeweils dargestellt, zwischen welchen Entitäten der beteiligten Kommunikationsinstanzen das jeweilige Kommunikationsprotokoll durchgeführt wird.

So wird, dargestellt mittels eines ersten Pfeils 106, zwischen der Kommunikationsnetzwerk-Domäne 102 und dem Zugangs-Router 105 ein Protokoll zum Bereitstellen der Kommunikationsnetzwerk-Domänen-Sicherheit bereitgestellt (1. Network Domain Security in Fig.1).

Ferner ist im Rahmen eines zweiten Kommunikationsprotokolls, dargestellt in Fig.1 mittels eines zweiten Pfeils 107, eine sichere IP-Adress-Konfiguration vorgesehen (2. Secure IP-Address-Configuration in Fig.1).

Unter Verwendung des Mobilfunk-Kommunikationsendgeräts 103, des Vermittlungsknotens 104 und des Zugangs-Routers 105 erfolgt eine Etablierung einer Authentifikations- und Sicherheitsbeziehung zwischen einerseits dem Mobilfunk-Kommunikationsendgerät 103 und dem Zugangs-Router 105 und andererseits zwischen dem Zugangs-Router 105 und der Kommunikationsnetzwerk-Domäne 102, in Fig.1 symbolisiert durch einen dritten Pfeil 108 und einem vierten Pfeil 109 (3. Authentication and Security Association Establishment in Fig.1).

Ferner sind üblicherweise Kommunikationsprotokolle auf der Ebene der Schicht 2 des OSI-Referenzmodells (OSI: **O**pen **S**ystems **I**nterconnection), d.h. zur Bereitstellung von Sicherheitsmechanismen auf der Ebene der Datensicherungsschicht, vorgesehen, in Fig.1 dargestellt mittels eines fünften Pfeils 110 zwischen dem Mobilfunk-Kommunikationsendgerät 103 und dem Vermittlungsknoten 104 bzw. mittels eines sechsten Pfeils 111 zur Sicherung der Kommunikation auf Datensicherungsschicht-Ebene zwischen dem Vermittlungsknoten 104 und dem Zugangs-Router 105.

Ein siebter Pfeil 112 symbolisiert ein weiteres Kommunikationsprotokoll zur Bereitstellung von Sicherheitsmechanismen auf Internet Protokoll-Schicht-Ebene zwischen dem Mobilfunk-Kommunikationsendgerät 103 und dem Zugangs-Router 105.

Von besonderer Bedeutung sind im Folgenden die Kommunikationsprotokolle zur sicheren IP-Adress-Konfiguration (symbolisiert mittels des zweiten Pfeils 107) und der Authentifikations- und Sicherheitsbeziehungs-Etablierung (symbolisiert mit-

tels des dritten Pfeils 108 bzw. mittels des vierten Pfeils 109).

Zur Bereitstellung von Konfigurationsparametern im Rahmen von Firmen-Kommunikationsnetzwerken ist es bekannt, diese entweder statisch oder dynamisch zu konfigurieren, beispielsweise gemäß dem **D**ynamic **H**ost **C**onfiguration **P**rotocol for IP**v6** (DHCPv6), wie in [2] oder in [3] beschrieben.

In [2] und [3] selbst ist kein kryptographischer Schutz der jeweiligen dort beschriebenen Kommunikationsprotokolle vorgesehen. Das DHCP bietet jedoch die Möglichkeit, die elektronischen Nachrichten des Kommunikationsprotokolls durch einen vorab ausgehandelten kryptographischen Schlüssel zu sichern. Diese Möglichkeit ist in [4] beschrieben.

Für den Zugang zu einem Internet-Service-Provider wird derzeit nahezu ausschließlich das Point-to-Point Protocol (PPP) oder eine Variation, bezeichnet als **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet (PPPoE), verwendet, um die erforderlichen Konfigurationsparameter an das Mobilfunk-Kommunikationsendgerät zu übermitteln.

Für einen Zugang zu einem virtuellen privaten Netzwerk (Virtual Private Network, VPN) ist es bekannt, zwei Protokolle zu verwenden, um die Konfigurationsparameter für das Mobilfunk-Kommunikationsendgerät, d.h. die Konfigurationsdaten kryptographisch geschützt zu transportieren, nämlich ein erstes Protokoll ModeConfig bzw. ein zweites Kommunikationsprotokoll DHCP, welche Protokolle in [5], [6], [7] und [8] beschrieben sind.

Bei dem Kommunikationsprotokoll ModeConfig wurden in das Authentifikations- und Schlüsselaushandlungsprotokoll Internet Key Exchange (IKE) (beschrieben in [9]) bzw. in das Internet Key Exchange v2 Protokoll (IKEv2), beschrieben in [10], integriert.

Um eine kryptographisch gesicherte Übertragung von Konfigurationsparametern zwischen dem Kommunikationsnetzwerk und einem Mobilfunk-Kommunikationsendgerät zu ermöglichen, wurden in der Vergangenheit unterschiedliche Verfahren benutzt.

Diese Verfahren lassen sich insbesondere in drei Gruppen aufteilen:

1. Erweiterungen zu DHCP:

   Um DHCP-Nachrichten im Umfeld der Mobilfunk-Kommunikationsgeräte kryptographisch zu schützen wurden eine Reihe von Erweiterungen zu DHCP vorgeschlagen, wie sie beispielsweise in [11], [12], [13] und [14] beschrieben sind.

   Diese Erweiterungen zu DHCP sollen es einem Mobilfunk-Kommunikationsendgerät ermöglichen, sich dynamisch in dem Kommunikationsnetzwerk eine Sicherheitsbeziehung mit dem DHCP-Server-Computer aufzubauen.

2. Erweiterungen von Extensible Authentication Protocol (EAP) Verfahren:

   Das Extensible Authentication Protocol ist in [16] beschrieben.

In [15] ist eine Erweiterung eines EAP-Verfahrens beschrieben, mit dem es ermöglicht ist, das Internet Key Exchange Protocol v2, wie es in [10] beschrieben ist, wiederzuverwenden.

Als ein Nebeneffekt besteht in IKEv2 die Möglichkeit, Konfigurationsparameter kryptographisch geschützt zu übertragen.

3. Bootstrapping-Methode:

Ferner ist ein Kommunikationsprotokoll-Vorschlag bekannt, mit dem die initiale Netzwerkauthentifikation unter Verwendung von EAP und die Bereitstellung einer Sicherheits-Kommunikationsverbindung mit dem DHCP-Server-Computer ermöglicht wird (vgl. [17]).

Der Vorteil dieses Verfahrens liegt in der Trennung zwischen der Netzwerkauthentifikation und der kryptographischen Sicherung der DHCP-Nachrichten.

Das DHCP-Kommunikationsprotokoll muss in diesem Fall nicht verändert werden.

In [18] ist ein Verfahren zur EAP-Authorisation beschrieben.

Weitere Erweiterungen zu dem Extensible Authentication Protocol zur kryptographisch gesicherten Datenübertragung sind in [19], [20] und [21] beschrieben.

Der Erfindung liegt das Problem zugrunde, auf einfache Weise Kommunikations-Konfigurationsdaten einem Kommunikationsgerät kryptographisch gesichert bereitzustellen.

Das Problem wird durch ein Verfahren und eine Einrichtung zum Bilden einer verschlüsselten Nachricht sowie durch ein Verfahren und eine Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen. Die im Folgenden beschriebenen Ausgestaltungen der Erfindung betreffen sowohl das Verfahren als auch die Einrichtung zum Bilden einer verschlüsselten Nachricht als auch das Verfahren und die Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht.

Die im Folgenden beschriebenen Komponenten der Erfindung können in Software, d.h. mittels eines Computerprogramms, in Hardware, d.h. mittels einer speziellen elektrischen Schaltung oder in beliebig hybrider Form, d.h. teilweise in Hardware und teilweise in Software, realisiert sein.

Bei einem Verfahren zum Bilden einer verschlüsselten Nachricht, wobei die verschlüsselte Nachricht Kommunikations-Konfigurationsdaten enthält, wird unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchgeführt, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar, aufweisend mindestens zwei kryptographisch zueinander korrespondierende Schlüssel, gebildet wird. Unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars werden die Kommunikations-

Konfigurationsdaten von der ersten Kommunikationseinheit verschlüsselt, womit die verschlüsselte Nachricht gebildet wird.

Bei einem Verfahren zum Entschlüsseln einer verschlüsselten Nachricht, welche verschlüsselte Nachricht Kommunikations-Konfigurations-Daten enthält, wird unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchgeführt, wodurch für die erste Kommunikationseinheit und für die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird. Unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars werden die in der verschlüsselten Nachricht enthaltenen Kommunikations-Konfigurationsdaten von der zweiten Kommunikationseinheit unter Entschlüsselung der verschlüsselten Nachricht ermittelt.

Eine Einrichtung zum Bilden einer verschlüsselten Nachricht, welche verschlüsselte Nachricht Kommunikations-Konfigurationsdaten enthält, weist eine Schlüsselerzeugungs-Einheit auf, welche eingerichtet ist, unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchzuführen, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird. Ferner weist die Einrichtung eine Verschlüsselungseinheit auf, welche eingerichtet ist, unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars die Kommunikations-Konfigurations-Daten

zu verschlüsseln, womit die verschlüsselte Nachricht gebildet wird.

Eine Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht, wobei die verschlüsselte Nachricht Kommunikations-Konfigurations-Daten enthält, weist eine Schlüsselerzeugungseinheit auf, welche eingerichtet ist, unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchzuführen, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird. Ferner weist die Einrichtung eine Entschlüsselungseinheit auf, welche eingerichtet ist, unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars Kommunikations-Konfigurations-Daten von der zweiten Kommunikationseinheit unter Entschlüsselung der verschlüsselten Nachricht, welche die Kommunikations-Konfigurations-Daten enthält, zu entschlüsseln.

Gemäß einer Ausgestaltung der Erfindung basiert das internet-basierte Authentifikationsverfahren auf einem Extensible Authentication Protocol-Verfahren.

Alternativ kann jedes Authentifikationsverfahren verwendet werden, bei dem ein kryptographisches Schlüsselpaar gebildet werden wird und welches unmittelbar die Dienste der Sicherungsschicht ohne Zwischenschaltung einer IP-Schicht in Anspruch genommen wird. Anschaulich bedeutet dies, dass das internet-basierte Authentifikationsverfahren auf Schicht-3-Ebene gemäß dem OSI-Referenzmodell, d.h. auf der Ebene der Vermittlungsschicht realisiert ist.

Anders ausgedrückt bedeutet dies, dass erfindungsgemäß standardisierte Konfigurationsprotokolle, wie sie beispielsweise in [5], [6], [7] oder [8] beschrieben sind, verwendet werden, um ein Kommunikationsendgerät, vorzugsweise ein Mobilfunk-Kommunikationsendgerät, zu konfigurieren, d.h. mit Konfigurationsdaten, im Folgenden auch bezeichnet als Kommunikations-Konfigurationsdaten bzw. Kommunikations-Konfigurationsparameter, zu versehen.

Dies geschieht in einer Art und Weise, die gemäß dem Stand der Technik nicht vorgesehen ist.

Anschaulich werden die standardisierten Konfigurationsprotokolle kryptographisch gesichert unter Verwendung kryptographischer Schlüssel, die mittels eines vorangegangenen internet-basierten Authentifikationsverfahrens, besonders bevorzugt einem vorangegangenen EAP-basierten Netzwerkauthentifikationsverfahren bzw. Netzwerkauthentifikationsmechanismus, gebildet wurden.

Anders ausgedrückt werden standardisierte Konfigurationsprotokolle, beispielsweise DHCP oder ModeConfig geschützt durch im Rahmen einer vorangegangenen Netzwerkzugangsauthentifikation gebildeter kryptographischer Schlüssel.

Die Kommunikations-Konfigurationsdaten können unter Verwendung von elektronischen Nachrichten gemäß dem internet-basierten Authentifikationsverfahren von der ersten Kommunikationseinheit zu der zweiten Kommunikationseinheit übertragen werden.

Diese Ausgestaltung der Erfindung weist insbesondere den Vorteil auf, dass schon das zur Authentifikation und zur Schlüsselerzeugung verwendete Kommunikationsprotokoll in den zu verwendenden Nachrichtenformaten auch zur Übertragung der Kommunikations-Konfigurationsdaten von dem Kommunikationsnetzwerk zu dem Kommunikationsendgerät verwendet werden kann, womit die Implementierung des erfindungsgemäßen Verfahrens erheblich vereinfacht wird.

Gemäß einer anderen Ausgestaltung der Erfindung ist es vorgesehen, dass die Kommunikations-Konfigurationsdaten unter Verwendung von elektronischen Nachrichten gemäß einem der vorliegenden internet-basierten Authentifikationsverfahren von der ersten Kommunikationseinheit zu der zweiten Kommunikationseinheit übertragen werden

- Protected Extensible Authentication Protocol-Verfahren,
- Extensible Authentication Protocol Tunneled TLS Authentication Protocol-Verfahren, oder
- Protocol for Carrying Authentication for Network Access-Verfahren.

Anders ausgedrückt bedeutet dies, dass die Übertragung der Kommunikations-Konfigurationsdaten gemäß dem in [20], dem in [21] oder gemäß dem in [17] beschriebenen Verfahren übertragen werden kann.

Wird das EAP-basierte Verfahren selbst zur Übertragung der Kommunikations-Konfigurationsdaten verwendet, so kann der Schutz der EAP-Konfigurationsnachrichten über an sich bekannte Tunneling-Methoden, wie sie beispielsweise in [20], in [21] oder in [17] beschrieben sind, oder durch EAP-interne Schutzmechanismen, beispielsweise gemäß [19] erfolgen. In diesem Zusammenhang ist es ebenfalls möglich, das in [18] be-

schriebene Verfahren als Container zu verwenden, um die Kommunikations-Konfigurationsdaten zu transportieren.

Vorzugsweise ist die erste Kommunikationseinheit eine Kommunikationseinheit eines Kommunikationsnetzwerk-Elements, besonders bevorzugt eine Kommunikationseinheit eines Kommunikationsnetzwerk-Elements in einem Mobilfunk-Kommunikationsnetzwerk, beispielsweise gemäß einem 3GPP-Mobilfunkstandard, beispielsweise einem Kommunikationsnetzwerkelement, welches gemäß UMTS eingerichtet ist, alternativ gemäß einem anderen Mobilfunkstandard, z.B. GSM, eingerichtet ist.

Gemäß einer anderen Ausgestaltung der Erfindung ist es vorgesehen, dass die zweite Kommunikationseinheit ein Kommunikationsendgerät ist, besonders bevorzugt ein Mobilfunk-Kommunikationsendgerät, beispielsweise eingerichtet gemäß einem Mobilfunk-Kommunikationsstandard gemäß 3GPP, beispielsweise gemäß dem UMTS-Kommunikationsstandard, alternativ gemäß dem GSM-Kommunikationsstandard.

Insbesondere im Rahmen der Übertragung von Konfigurationsdaten zu einem Mobilfunk-Kommunikationsendgerät über eine Luftschnittstelle eignet sich die oben beschriebene Vorgehensweise, da die in diesem Zusammenhang standardisierten Kommunikationsprotokollen sehr einfach und kostengünstig verwendet werden können zum sicheren Übertragen der Kommunikations-Konfigurationsparameter aus einer Kommunikationsnetzwerk-Domäne hin zu einem Mobilfunk-Kommunikationsendgerät.

Gemäß einer anderen Ausgestaltung der Erfindung ist es vorgesehen, dass die Kommunikations-Konfigurationsdaten gemäß einem Protokollformat eines Protokolls zum Konfigurieren eines

Kommunikationsendgeräts codiert sind, vorzugsweise gemäß einem Protokollformat eines Protokolls zum dynamischen Konfigurieren eines Kommunikationsendgeräts, besonders bevorzugt gemäß einem Protokollformat eines Dynamical Host Configuration Protocols zum dynamischen Konfigurieren eines Kommunikationsendgeräts, wie es beispielsweise in [2] beschrieben ist.

Insbesondere bei einem EAP-basierten Authentifikationsverfahren zeichnet sich die Verwendung der im Rahmen des EAP-basierten Authentifikationsverfahrens erzeugte kryptographische Schlüsselmaterial zur kryptographisch gesicherten Übertragung der Kommunikations-Konfigurationsdaten im Rahmen eines DHCP-Kommunikationsprotokolls oder ModeConfig-Kommunikationsprotokolls durch die Einfachheit und damit die kostengünstige Realisierbarkeit aus.

Unter Kommunikations-Konfigurationsdaten sind in diesem Zusammenhang alle Daten oder Parameter zu verstehen, mittels welcher Kommunikations-Eigenschaften des Kommunikationsendgeräts im Rahmen einer Kommunikationssitzung charakterisiert werden.

Beispielsweise sind unter Kommunikations-Konfigurationsdaten eine mittels des Konfigurationsprotokolls, vorzugsweise gemäß dem Dynamical Host Configuration Protocol vorgesehene Daten zum Charakterisieren des Kommunikationsendgeräts, beispielsweise die gemäß dem BOOTP vorgesehenen Informationen, die ein auf den BOOTP-basierenden Server-Computer bereitgestellt werden, insbesondere die IP-Adresse des Kommunikationsendgeräts, eine so genannte Subnetz-Maske, eine IP-Adresse des Default Gateways, eine IP-Adresse des primären DNS-Servers und/oder des sekundären DNS-Servers, eine IP-Adresse des primären WINS-Servers oder einer IP-Adresse des sekundären WINS-

Servers, eine Pfadangabe zu der erforderlichen BOOTP-Datei, ein Kommunikationsnetzwerk-Domänen-Suffix des Clients, d.h. des Mobilfunk-Kommunikationsendgeräts, einer IP-Adresse des eines Zeitserver-Computers sowie ein Zeit-Offset von der Coordinated Universal Time (CMT).

Ausführungsbeispiele der Erfindung sind in den Figuren dargestellt und werden im Folgenden näher erläutert.

Es zeigen

Figur 1 eine Kommunikationsanordnung gemäß dem Stand der Technik;

Figuren 2a bis 2d ein Nachrichtenflussdiagramm, in dem die einzelnen Verfahrensschritte zum Übermitteln von Kommunikations-Konfigurationsdaten gemäß einem ersten Ausführungsbeispiel der Erfindung dargestellt sind; und

Figur 3a und 3b ein Nachrichtenflussdiagramm, in dem die einzelnen Verfahrensschritte zum Übermitteln von Kommunikations-Konfigurationsdaten gemäß einem zweiten Ausführungsbeispiel der Erfindung dargestellt sind.

**Fig.2a** bis **Fig.2d** zeigt ein Nachrichtenflussdiagramm 200, in dem der Austausch von elektronischen Nachrichten zwischen Einheiten eines Mobilfunk-Kommunikationssystems, eingerichtet gemäß dem UMTS-Kommunikationsstandard, dargestellt ist. Insbesondere sind in den Fig.2a bis Fig.2d dargestellt ein Mobilfunk-Kommunikationsendgerät 201, ein Wireless Local Area Network (WLAN) Zugangsknoten-Rechner 202, ein TTLS-Server-Rechner 203 sowie eine **A**uthorization **A**uthentication and **A**ccounting-Einheit 204 (AAA-Einheit).

Die weiteren üblichen Komponenten des Mobilfunk-Kommunikationsnetzwerks gemäß dem UMTS-Standard, insbesondere die Einheiten des Kernnetzwerks sowie die weiteren Mobilfunk-Kommunikationsendgeräte oder Festnetz-Kommunikationsendgeräte, welche in dem Kommunikationssystem zum Bereitstellen einer Kommunikationsverbindung ebenfalls vorgesehen sind, sind aus Gründen der Einfachheit in dem Nachrichtenflussdiagramm 200 von Fig.2a bis Fig.2d nicht dargestellt.

Das Kommunikationssystem ist hinsichtlich des Nachrichtenflusses eingerichtet wie in [21] beschrieben mit der im Folgenden beschriebenen erfindungsgemäßen Erweiterung.

Zunächst wird somit das in [21] beschriebene Verfahren durchgeführt zum Aufbau eines TLS-Tunnels, wobei eine einseitige Authentifikation des Server-Rechners 204 zu dem Client-Rechner gemäß diesem Ausführungsbeispiel zu dem Mobilfunk-Kommunikationsendgeräts 201 durchgeführt wird. Der Nachrichtenfluss entspricht im Wesentlichen dem in [21] in Abschnitt 13.2 beschriebenen.

Nach erfolgtem Aufbau des TLS-Tunnels, wie er nachfolgend noch näher erläutert wird, wird eine EAP/MD5-Challenge-Authentifikation, d.h. anders ausgedrückt eine einseitige Authentifikation des Client-Rechners, gemäß diesem Ausführungsbeispiel des Mobilfunk-Kommunikationsendgeräts 201, zu dem Server-Rechner 204 durchgeführt.

Wie in [21] beschrieben, beginnt das Verfahren damit, dass der Zugangspunkt-Knotenrechner 202 gemäß [21] eine Extensible Authentification Protocol-Request/Identity-Nachricht 205 bil-

det und an das Mobilfunk-Kommunikationsendgerät 201 übermittelt.

In Reaktion darauf bildet und sendet das Mobilfunk-Kommunikationsendgerät 201 eine EAP-Response/Identity-Nachricht 206 an den Zugangspunkt-Knotenrechner 202, welcher auf den Empfang dieser Nachricht 206 hin eine RADIUS Access-Request-Nachricht 207 mit den Nachrichten-Parametern „XXX-Data-Cipher-Suite+" und „EAP-Response passthrough" bildet und an den TTLS-Server-Rechner 203 übermittelt.

Auf dem Empfang der RADIUS Access-Request-Nachricht 207 hin bildet und übermittelt der TTLS-Server-Rechner 203 eine RADIUS Access-Challenge-Nachricht 208 mit dem Parameter EAP-Request/TTLS-Start an den Zugangspunkt-Knotenrechner 202.

Nach Empfang der Nachricht 208 bildet der Zugangspunkt-Knotenrechner 202 eine EAP-Request passthrough-Nachricht 209 und sendet diese zu dem Mobilfunk-Kommunikationsendgerät 201.

Nach Empfang der Nachricht 209 bildet das Mobilfunk-Kommunikationsendgerät 201 eine EAP-Response/TTLS-Nachricht 210 mit dem Parameter „ClientHello" als Nutzdatenelement und sendet diese Nachricht 210 an den Zugangspunkt-Knotenrechner 202.

Der Zugangspunkt-Knotenrechner 202 wiederum bildet auf Empfang der Nachricht 210 hin eine RADIUS Access-Request-Nachricht 211 mit dem Parameter „EAP-Response passthrough" als Nutzdatenelement und sendet diese Nachricht 211 zu dem TTLS-Server-Rechner 203.

Nachdem der TTLS-Server-Rechner 203 die RADIUS Access-Request-Nachricht 211 empfangen hat und das Nutzdatenelement EAP-Response passthrough ausgewertet hat, bildet der TTLS-Server-Rechner 203 eine RADIUS Access-Challenge-Nachricht 212 und sendet diese an den Zugangspunkt-Knotenrechner 202. In der RADIUS Access-Challenge-Nachricht 212 sind als Nutzdatenelemente, d.h. als Nachrichtenparameter enthalten: „EAP-Request-TTLS", „ServerHello", „Certificate", „ServerKeyExchange" und „ServerHelloDone".

Wie in **Fig.2b** dargestellt ist, übermittelt der Zugangspunkt-Knotenrechner 202 auf den Empfang der Nachricht 212 hin eine von ihm gebildete EAP-Request passthrough-Nachricht 213 an das Mobilfunk-Kommunikationsendgerät 201, welches daraufhin gemäß dem in [21] beschriebenen Verfahren eine EAP-Response/TTLS-Nachricht 214 mit den Parametern „ClientKeyExchange", „Change-Cipher-Spec", „Finished" als Nachrichtenparameter und sendet die Nachricht 214 zu dem Zugangspunkt-Knotenrechner 202, welcher auf dem Empfang der Nachricht 214 hin eine RADIUS Access-Request-Nachricht 215 mit dem Nachrichtenparameter „EAP-Response passthrough" bildet und diese an den TTLS-Server-Rechner 203 übermittelt.

Der TTLS-Server-Rechner 203 bildet auf den Empfang der Nachricht 215 hin eine RADIUS Access-Challenge-Nachricht 216 mit den folgenden Nachrichtenparametern: „EAP-Request/TTLS", „Change-Cipher-Spec", „Finished", und sendet die Nachricht 216 zu dem Zugangspunkt-Knotenrechner 202, welcher auf den Empfang der Nachricht 216 hin eine EAP-Request passthrough-Nachricht 217 bildet und diese zu dem Mobilfunk-Kommunikationsendgerät 201 übermittelt.

Nach Empfang der Nachricht 217 bildet in Reaktion darauf das Mobilfunk-Kommunikationsendgerät 201 eine EAP-Response/TTLS-Nachricht 218 mit den Parametern „{EAP-Response/Identity}" und „{XXX-Data-Cipher-Suite+}" und sendet die Nachricht 218 zu den Zugangspunktsknotenrechner 202.

Der Zugangspunkt-Knotenrechner 202 wiederum bildet auf Empfang der Nachricht 218 hin eine RADIUS Access-Request-Nachricht 219 mit dem Element „EAP-Response passthrough". Die Nachricht 219 wird von dem Zugangspunkt-Knotenrechner 202 zu dem TTLS-Server-Rechner 203 übertragen, welcher auf dem Empfang der Nachricht 219 hin eine RADIUS Access-Request-Nachricht 220 mit der Angabe „EAP-Response/Identity" als Nutzdatenelement und sendet die Nachricht 220 zu dem AAA-Server-Rechner 204, welcher auf den Empfang der Nachricht 220 mit dem Bilden einer RADIUS Access-Challenge-Nachricht 221 reagiert, welche Nachricht als Parameter eine „EAP-Request/MD5-Challenge"-Angabe enthält (vgl. **Fig.2c**).

Die Nachricht 221 wird von dem AAA-Server-Rechner 204 zu dem TTLS-Server-Rechner 203 übertragen, welcher seinerseits auf den Empfang der Nachricht 221 hin eine RADIUS Access-Challenge-Nachricht 222 bildet, welche als Nachrichtenelemente eine „EAP-Request/TTLS"-Angabe enthält sowie als weitere Parameter „{EAP-Request/MD5-Challenge}" und „{XXX-Data-Cipher-Suite}".

Die Nachricht 222 wird von dem TTLS-Server-Rechner 203 zu dem Zugangspunkt-Knotenrechner 202 übertragen, welcher auf den Empfang der Nachricht 222 hin eine EAP-Request passthrough-Nachricht 223 bildet und zu dem Mobilfunk-Kommunikationsendgerät überträgt.

Von dem Mobilfunk-Kommunikationsendgerät 201 wird auf den Empfang der Nachricht 223 hin eine EAP-Response/TTLS-Nachricht 224 mit der Angabe „{EAP-Response/MD5-Challenge}" gebildet und zu dem Zugangspunkt-Knotenrechner 202 übertragen, welche auf den Empfang dieser Nachricht hin eine RADIUS Access-Request-Nachricht 225 mit EAP-Response passthrough bildet und zu dem TTLS-Server-Rechner 203 übermittelt.

Auf den Empfang der Nachricht 225 hin bildet der TTLS-Server-Rechner 203 eine RADIUS Access-Challenge-Nachricht 226 mit der Angabe EAP-Response/MD5-Challenge und übermittelt die Nachricht 226 an den AAA-Server-Rechner 204.

Der AAA-Server-Rechner 204 bildet auf den Empfang der Nachricht 226 hin eine RADIUS Access-Accept-Nachricht 227 und sendet diese zu dem TTLS-Server-Rechner 203, welcher auf dem Empfang der Nachricht 227 hin eine weitere RADIUS Access-Accept-Nachricht 228 mit folgenden Nachrichtenparametern bildet: „XXX-Data-Cipher-Suite", „XXX-Data-Keying-Material", „EAP-Success". Die Nachricht 228 wird von dem TTLS-Server-Rechner 203 zu dem Zugangspunkt-Knotenrechner 202 übertragen, welcher auf den Empfang der Nachricht 228 hin eine EAP-Success passthrough-Nachricht 229 bildet und an das Mobilfunk-Kommunikationsendgerät 201 übermittelt, womit eine gegenseitige Authentifikation des Mobilfunk-Kommunikationsendgerätes und dem AAA-Server-Rechner, d.h. dem Netzwerk, erreicht ist.

Um Kommunikations-Konfigurationsdaten zu erhalten, übermittelt das Mobilfunk-Kommunikationsendgerät 201 eine Konfigurations-Anfragenachricht gemäß dem DHCP-Protocol als CP(CFG_REQUEST) als Nutzdatenelement innerhalb des in [21] beschriebenen Protokollformats in einer EAP-Response/TTLS-

Nachricht 230 und überträgt die Nachricht zu dem Zugangspunkt-Knotenrechner 202, welcher auf dem Empfang der Konfigurationsanfrage hin, wiederum unter Verwendung des in [21] beschriebenen Nachrichtenformats eine RADIUS Access-Request-Nachricht 231 bildet. Als Nachrichtenparameter weist die Nachricht 231 auf ein EAP-Response/TTLS passthrough mit zusätzlich der Angabe gemäß dem DHCP-Nachrichtenelement CP(CFG_REQUEST) (vgl. **Fig.2d**).

Die von dem Zugangspunkt-Knotenrechner 202 zu dem TTLS-Server-Rechner übertragene Nachricht 231 bringt den TTLS-Server 203 dazu, die für das Mobilfunk-Kommunikationsendgerät 201 verfügbaren und vorgesehenen Konfigurationsdaten, gemäß diesem Ausführungsbeispiel insbesondere eine oder mehrere dynamische(n) IP-Adresse(n) und übermittelt diese unter Verwendung der im Rahmen des Authentifikationsverfahrens, wie oben beschrieben, gebildeten Schlüsselmaterials in einer RADIUS Access-Challenge-Nachricht 232, welche als Nachrichtenparameter eine EAP-Request/TTLS mit den zusätzlichen Parametern gemäß dem DHCP-Protocol „CP(CFG_REPLY)" und sendet diese zu dem Zugangspunkt-Knotenrechner 202.

Der Zugangspunkt-Knotenrechner 202 wiederum ermittelt aus der Nachricht 232 die in den Nutzdaten CP(CFG_REPLY) enthaltenen Konfigurationsdaten, insbesondere die dynamische(n) IP-Adresse(n), welche für das Mobilfunk-Kommunikationsendgerät vorgesehen ist/sind und sendet die Konfigurationsdaten in Form des DHCP-Nachrichtenelements „CP(CFG_REPLY)", eingepackt in einer EAP-Response/TTLS-Nachricht 233, an das Mobilfunk-Kommunikationsendgerät 201.

Ist die Nachricht 233 erfolgreich zu dem Mobilfunk-Kommunikationsendgerät 201 übertragen worden, so ermittelt

dieses die Konfigurationsdaten aus der Nachricht 233 und verwendet diese wie in dem Steuerungsprogramm des Mobilfunk-Kommunikationsendgeräts 201 vorgesehen.

Anschaulich erfolgt somit die Übertragung der Mobilfunk-Kommunikations-Konfigurationsdaten nach erfolgter Beendigung der Authentifikation gemäß dem in [21] beschriebenen EAP-basierten Authentifikationsverfahren. Zusätzlich zu dem in [21] beschriebenen Verfahren ist eine Einrichtung der Rechner gemäß [7] vorgesehen, um dem Mobilfunk-Kommunikationsendgerät 201 als Client-Rechner die Möglichkeit zu geben, die Kommunikations-Konfigurationsdaten mittels der CFG_REQUEST-Nachricht anzufordern und mittels der CFG_REPLY-Nachricht zu erhalten.

Bis auf die in [7] proprietär beschriebenen Nachrichtenformate entspricht die Nomenklatur und die Einrichtung sowie die Parameter dem üblichen DHCP-Format, wie es beispielsweise in [3] beschrieben ist.

Die Übertragung der Kommunikations-Konfigurationsdaten erfolgt somit kryptographisch gesichert durch den aufgebauten TLS-Tunnel.

In dem Ausführungsbeispiel ist die Kommunikation zwischen dem TTLS-Server-Rechner 203 und dem Knoten, der die Konfigurationsdaten bereitstellt, beispielsweise einem DHCP-Server oder auch einem LDAP-Server, aus Gründen einer übersichtlicheren Darstellung der Erfindung nicht näher beschrieben.

In einer alternativen Ausführungsform ist es vorgesehen, dass die Kommunikations-Konfigurationsdaten unmittelbar nach Beendigung der gegenseitigen Authentifikation, beispielsweise

schon innerhalb der EAP-Success-Nachricht 229 an das Mobilfunk-Kommunikationsendgerät 201 übertragen wird.

Ein drittes Ausführungsbeispiel der Erfindung ist in einem Nachrichtenflussdiagramm 300 in den **Fig.3a** und **Fig.3b** dargestellt.

Das EAP-basierte Authentifikationsverfahren ist gemäß diesem Ausführungsbeispiel gemäß dem PANA-Verfahren, wie es in [17] beschrieben ist, ausgebildet.

Gemäß dem in [17] beschriebenen Protokoll wird von dem PANA-Client-Rechner 301 eine PANA_Discover(0,0)-Nachricht 303 gebildet und an den PAA-Server-Rechner 302 übermittelt, welcher auf den Empfang der PANA_Discover(0,0)-Nachricht 303 hin eine Antwortnachricht PANA_start(x,0)[Cookie]-Nachricht 304 bildet und dem Client-Rechner 301 übermittelt (vgl. **Fig.3a**).

Der PANA-Client-Rechner 301 bildet auf den Empfang der Nachricht 304 hin eine PANA_start(x,y)[Cookie]-Nachricht 305 und übermittelt diese an den PAA-Server-Rechner 302, welcher auf den Empfang der Nachricht 305 im Rahmen des EAP-basierten Authentifikationsverfahrens reagiert mit einer ersten Authentifikationsnachricht 306 PANA_auth(x+1,y)[EAP{Request}], welche zu dem Client-Rechner 301 übertragen wird.

Der Client-Rechner 301 bildet auf den Empfang der Nachricht 306 hin eine zweite Authentifikationsnachricht 307 PANA_auth(y+1,x+1)[EAP{Response}]. Die Nachricht 307 wird zu dem PAA-Server-Rechner 302 übertragen.

Nach Empfang der Nachricht 307 wird von dem PAA-Server-Rechner 302 eine dritte Authentifikationsnachricht 308

PANA_auth(x+2,y+1)[EAP{Request}] gebildet und zu dem Client-Rechner 301 übermittelt, welcher seinerseits auf den Empfang der Nachricht 308 hin eine vierte Authentifikationsnachricht 309 PANA_auth(y+2,x+2)[EAP{Response}] bildet und zu dem PAA-Server-Rechner übermittelt, womit die Sicherheitsbeziehung (PANA Security Association) etabliert ist.

Diese Vorgehensweise entspricht der in [17] beschriebenen.

Nachfolgend wird, wie in [17] ebenfalls beschrieben, von dem PAA-Server-Rechner 302 eine PANA-Bestätigungsnachricht 310 PANA_Success(x+3,y+2)[EAP{Success}, Device-Id, Data-Protection, MAC] gebildet und zu dem Client-Rechner 301 übermittelt, welcher vorzugsweise als Mobilfunk-Kommunikationsendgerät eingerichtet ist (vgl. **Fig.3b**).

Der Client-Rechner 301 bildet auf den Empfang der Nachricht 310 hin eine PANA-Success-Bestätigungsnachricht 311 PANA_Success_ack(y+3,x+3)[Device-Id, Data-Protection, CP (CFG_Request), MAC] und sendet diese zu dem PAA-Server-Rechner 302, welcher seinerseits auf den Empfang der Nachricht 311 hin eine weitere PANA-Nachricht 312 mit den angeforderten Konfigurationsdaten bildet und zu dem Client-Rechner 301 übermittelt als PANA_msg(x+4,y+3)[CP(CFG_Reply), MAC].

Anschaulich entspricht die Ausführungsform dem PANA-Protokoll gemäß [17] mit der Erweiterung, dass die Payloads zum Transport der Adresskonfigurationsnachrichten gemäß dem DHCP, alternativ gemäß ModeConfig, erfindungsgemäß erweitert sind.

In den Fig.3a und Fig.3b wurden ohne Einschränkung der Allgemeingültigkeit wiederum die Payloads gemäß [7] als Konfigurationspayloads verwendet.

Die Anfrage und die Antwort zum Erhalt der Kommunikations-Konfigurationsdaten wird durch den MAC-Payload, der durch eine Keyde-Message Digestfunktion realisiert wird, kryptographisch geschützt.

Die benötigten kryptographischen Schlüssel und Sicherheitsparameter, d.h. das kryptographische Schlüsselmaterial bzw. Sicherheitsmaterial werden durch die PANA-Security Association (SA) bereitgestellt, die mittels der EAP-Authentifikation, wie oben beschrieben und in [17] im Detail ausgeführt, erzeugt wurden.

In diesem Dokument sind folgende Veröffentlichungen zitiert:

[1] N. Prigent et al., DHCPv6 Threads, Internet-Draft, Mai 2001;

[2] C. Schäfer, Das DHCP-Handbuch, Ein Leitfaden zur Planung, Einführung und Administration von DHCP, Edison-Wesley-Verlag, ISBN 3-8273-1904-8, Seiten 141-149, 2002;

[3] R. Droms, Dynamic Host Configuration Protocol, Request for Comments: 2131, März 1997;

[4] R. Droms et al., Authentication for DHCP Messages, Request for Comments : 3118, Juni 2001 ;

[5] M. Richardson, A Method for Configuration for IPsec Clients Using DHCP, Internet-Draft, Februar 2003;

[6] T. Kivinen, DHCP over IKE, Internet-Draft, April 2003;

[7] D. Dukes, Configuration Payload, Internet-Draft, Juli 2003;

[8] D. Dukes et al., The ISAKMP Configuration Method, Internet-Draft, September 2001,

[9] D. Harkins et al., The Internet Key Exchange (IKE), Request for Comments: 2409, November 1998;

[10] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, Internet-Draft, April 2003;

[11] A. McAuley et al., Dynamic Registration and Configuration Protocol (DRCP), Internet-Draft, Januar 2001;

[12] B. Mukherjee et al., Extensions to DHCT for Roaming Users, Internet-Draft, Mai 2001;

[13] S. Medvinsky et al., Kerberos V Authentication Mode for Uninitialized Clients, Internet-Draft, Juli 2000;

[14] V. Gupta, Flexible Authentication for DHCP Messages, Internet-Draft, Februar 2003;

[15] H. Tschofenig et al., EAP IKEv2 Method, Internet-Draft, Februar 2004;

[16] L. Blunk et al., Extensible Authentication Protocol (EAP), Internet-Draft, Februar 2004;

[17] D. Forsberg et al., Protocol for Carrying Authentication for Network Access (PANA), Internet-Draft, Mai 2004;

[18] M. Grayson et al., EAP Authorisation, Internet-Draft, März 2003;

[19] T. Hiller et al., A Container Type for the Extensible Authentication Protocol (EAP), Internet-Draft, Mai 2003;

[20] H. Andersson et al., Protected EAP Protocol, Internet-Draft, Februar 2002

[21] P. Funk, EAP Tunnel TLS Authentication Protocol (EAP-PTLS), Internet-Draft, April 2004

Patentansprüche

1. Verfahren zum Bilden einer verschlüsselten Nachricht, welche Kommunikations-Konfigurationsdaten enthält,

- bei dem unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchgeführt wird, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird,
- bei dem unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars die Kommunikations-Konfigurationsdaten von der ersten Kommunikationseinheit verschlüsselt werden, womit die verschlüsselte Nachricht gebildet wird.

2. Verfahren gemäß Anspruch 1,
bei dem das internet-basierte Authentifikationsverfahren auf einem Extensible Authentication Protocol-Verfahren basiert.

3. Verfahren gemäß Anspruch 1 oder 2,
bei dem die Kommunikations-Konfigurationsdaten unter Verwendung von elektronischen Nachrichten gemäß dem internet-basierten Authentifikationsverfahren von der ersten Kommunikationseinheit zu der zweiten Kommunikationseinheit übertragen werden.

4. Verfahren gemäß einem der Ansprüche 1 bis 3,
bei dem die Kommunikations-Konfigurationsdaten unter Verwendung von elektronischen Nachrichten gemäß einem der folgenden internet-basierten Authentifikationsverfahren von der ersten Kommunikationseinheit zu der zweiten Kommunikationseinheit übertragen werden:

- Protected Extensible Authentication Protocol-Verfahren,
- Extensible Authentication Protocol Tunneled TLS Authentication Protocol-Verfahren, oder

- Protocol for Carrying Authentication for Network Access-Verfahren.

5. Verfahren gemäß einem der Ansprüche 1 bis 4,
bei dem die erste Kommunikationseinheit eine Kommunikationseinheit eines Kommunikationsnetzwerk-Elements ist.

6. Verfahren gemäß Anspruch 5,
bei dem die erste Kommunikationseinheit eine Kommunikationseinheit eines Kommunikationsnetzwerk-Elements in einem Mobilfunk-Kommunikationsnetzwerks ist.

7. Verfahren gemäß einem der Ansprüche 1 bis 6,
bei dem die zweite Kommunikationseinheit ein Kommunikationsendgerät ist.

8. Verfahren gemäß Anspruch 7,
bei dem die zweite Kommunikationseinheit ein Mobilfunk-Kommunikationsendgerät ist.

9. Verfahren gemäß einem der Ansprüche 1 bis 8,
bei dem die Kommunikations-Konfigurationsdaten gemäß einem Protokollformat eines Protokolls zum Konfigurieren eines Kommunikationsendgeräts codiert sind.

10. Verfahren gemäß Anspruch 9,
bei dem die Kommunikations-Konfigurationsdaten gemäß einem Protokollformat eines Protokolls zum dynamischen Konfigurieren eines Kommunikationsendgeräts codiert sind.

11. Verfahren gemäß Anspruch 10,
bei dem die Kommunikations-Konfigurationsdaten gemäß einem Protokollformat eines Dynamic Host Configuration Protokolls zum dynamischen Konfigurieren eines Kommunikationsendgeräts codiert sind.

12. Verfahren zum Entschlüsseln einer verschlüsselten Nachricht, welche Kommunikations-Konfigurationsdaten enthält,

- bei dem unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchgeführt wird, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird,
- bei dem unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars Kommunikations-Konfigurationsdaten von der zweiten Kommunikationseinheit unter Entschlüsselung der verschlüsselten Nachricht, welche die Kommunikations-Konfigurationsdaten enthält, ermittelt werden.

13. Einrichtung zum Bilden einer verschlüsselten Nachricht, wobei die verschlüsselte Nachricht Kommunikations-Konfigurationsdaten enthält,

- mit einer Schlüsselerzeugungs-Einheit, welche eingerichtet ist, unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchzuführen, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird,
- mit einer Verschlüsselungseinheit, welche eingerichtet ist, unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars die Kommunikations-Konfigurationsdaten zu verschlüsseln, womit die verschlüsselte Nachricht gebildet wird.

14. Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht, wobei die verschlüsselte Nachricht Kommunikations-Konfigurationsdaten enthält,

- mit einer Schlüsselerzeugungs-Einheit, welche eingerichtet ist, unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchzuführen, wodurch für die erste Kommunikationseinheit und die zweite Kommunikationseinheit mindestens ein kryptographisches Schlüsselpaar gebildet wird,
- mit einer Entschlüsselungseinheit, welche eingerichtet ist, unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars Kommunikations-Konfigurationsdaten von der zweiten Kommunikationseinheit unter Entschlüsselung der verschlüsselten Nachricht, welche die Kommunikations-Konfigurationsdaten enthält, zu entschlüsseln.

FIG 1

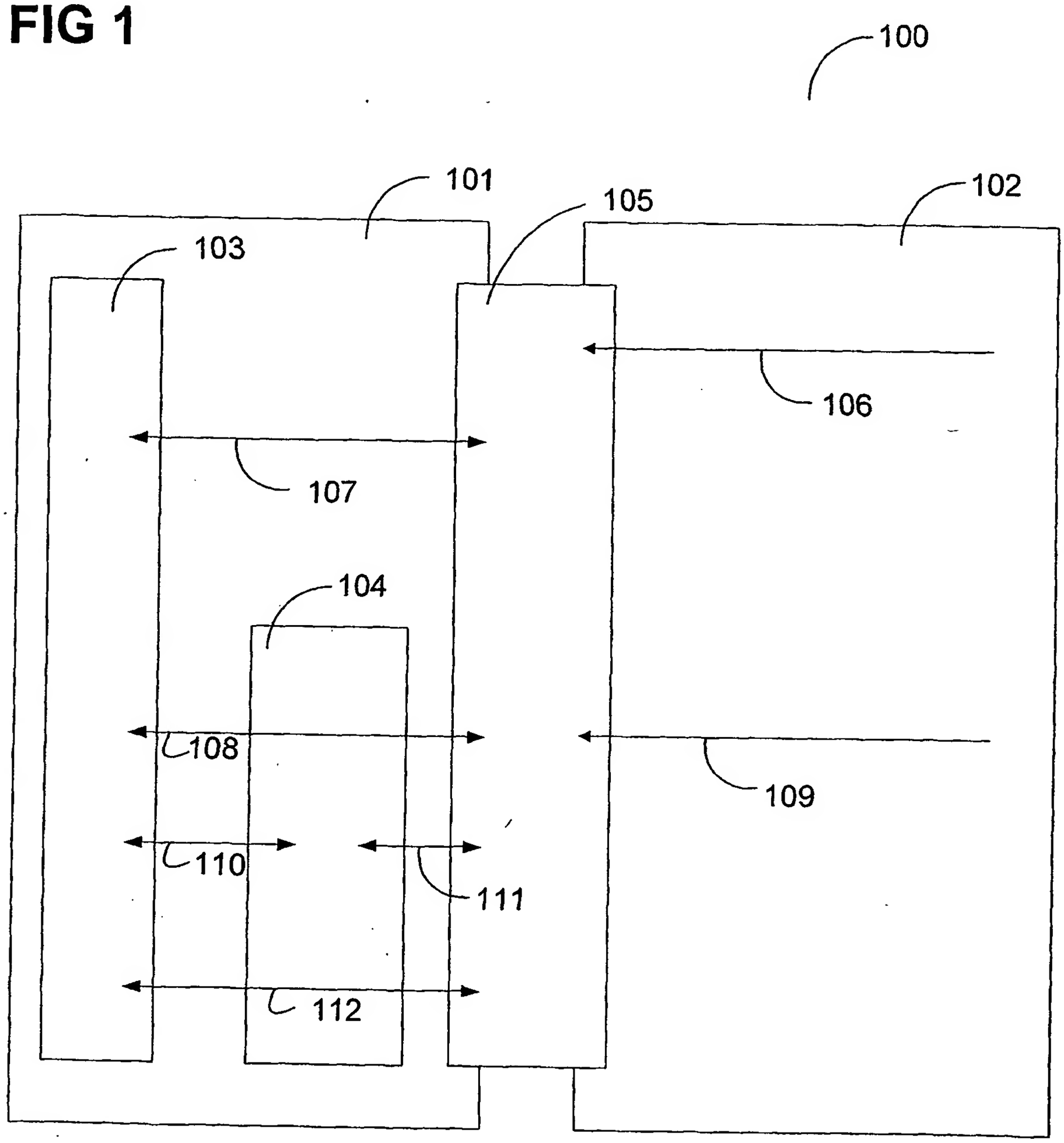


FIG 2A

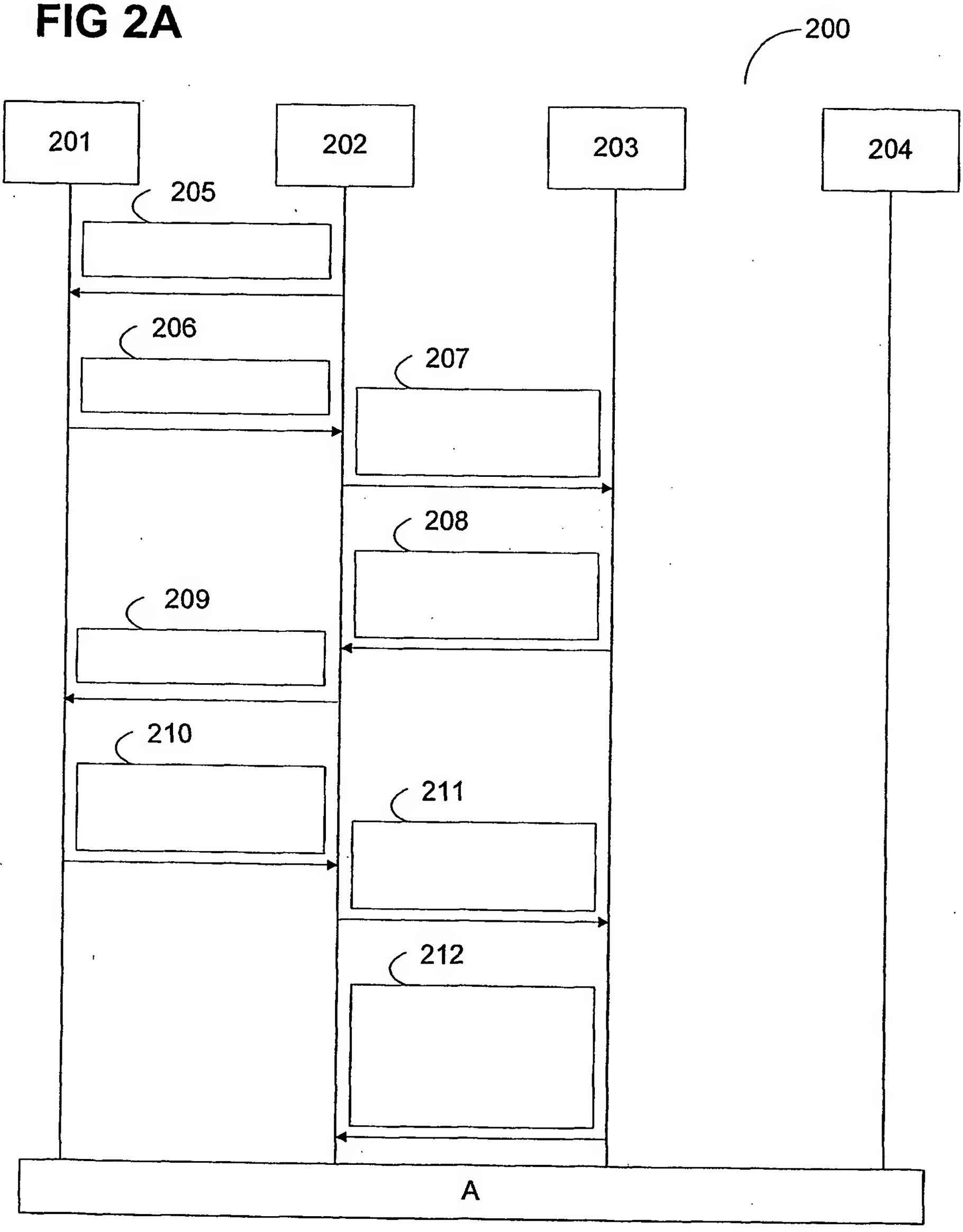


FIG 2B

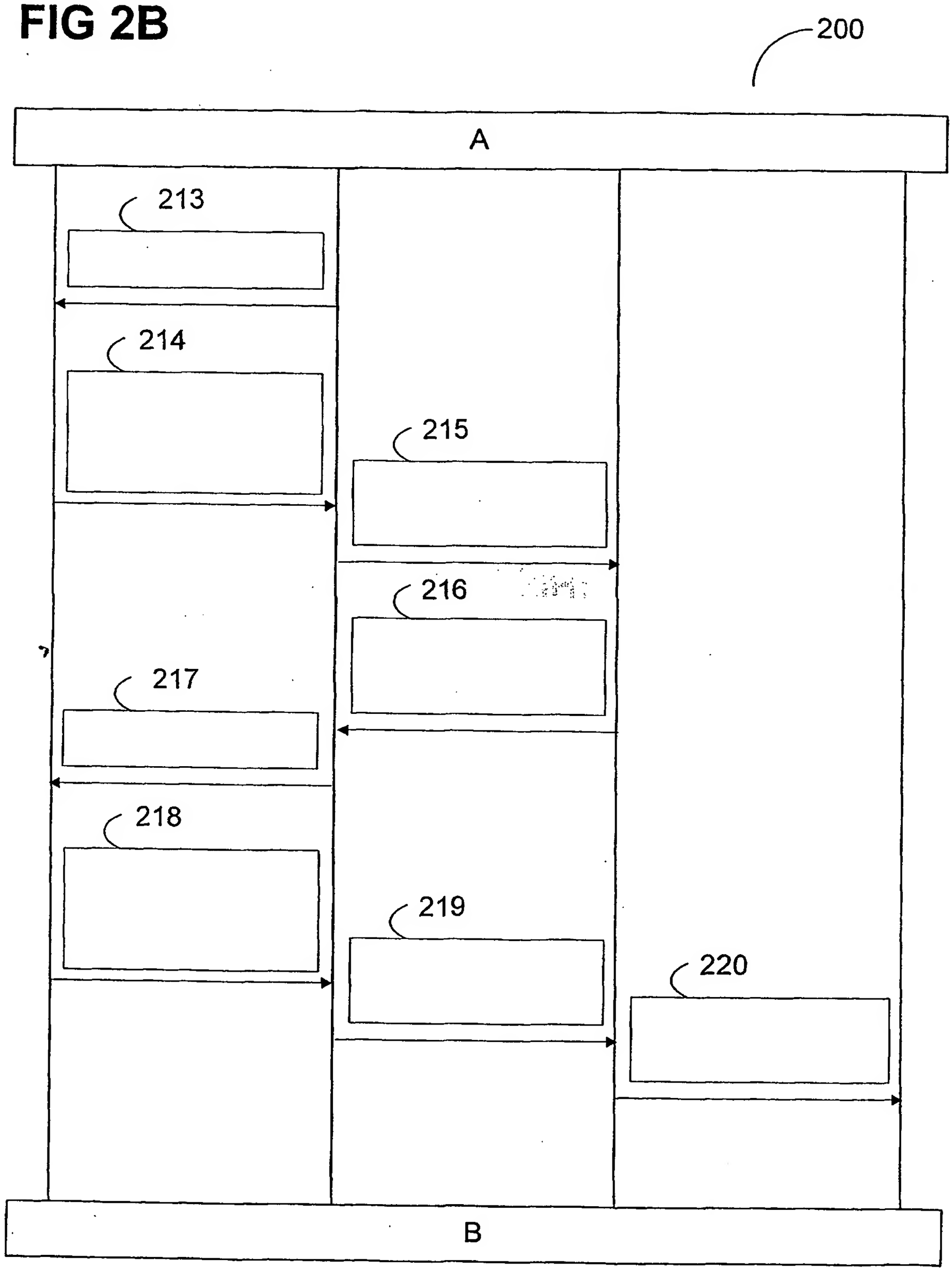


FIG 2C

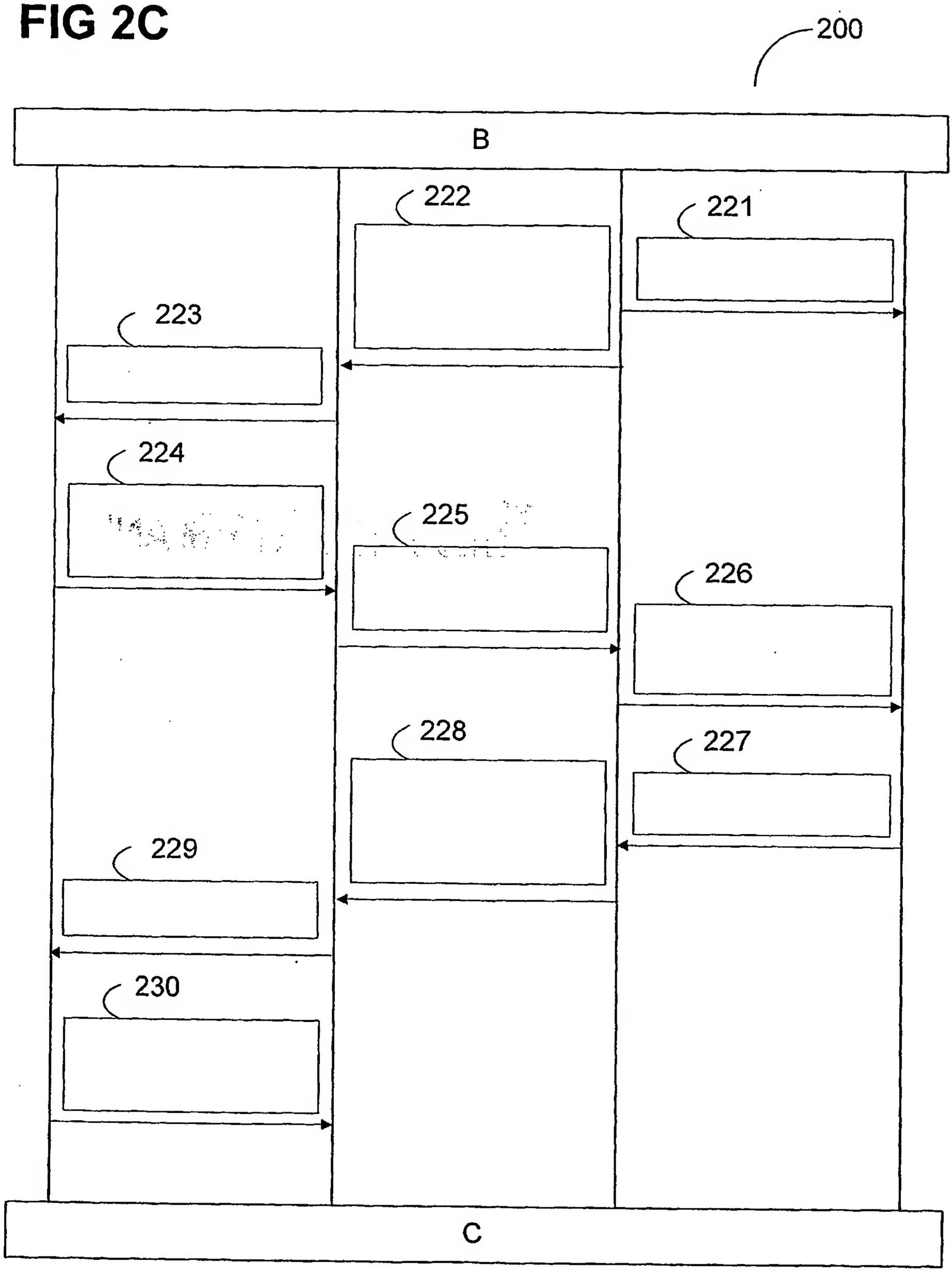


FIG 2D

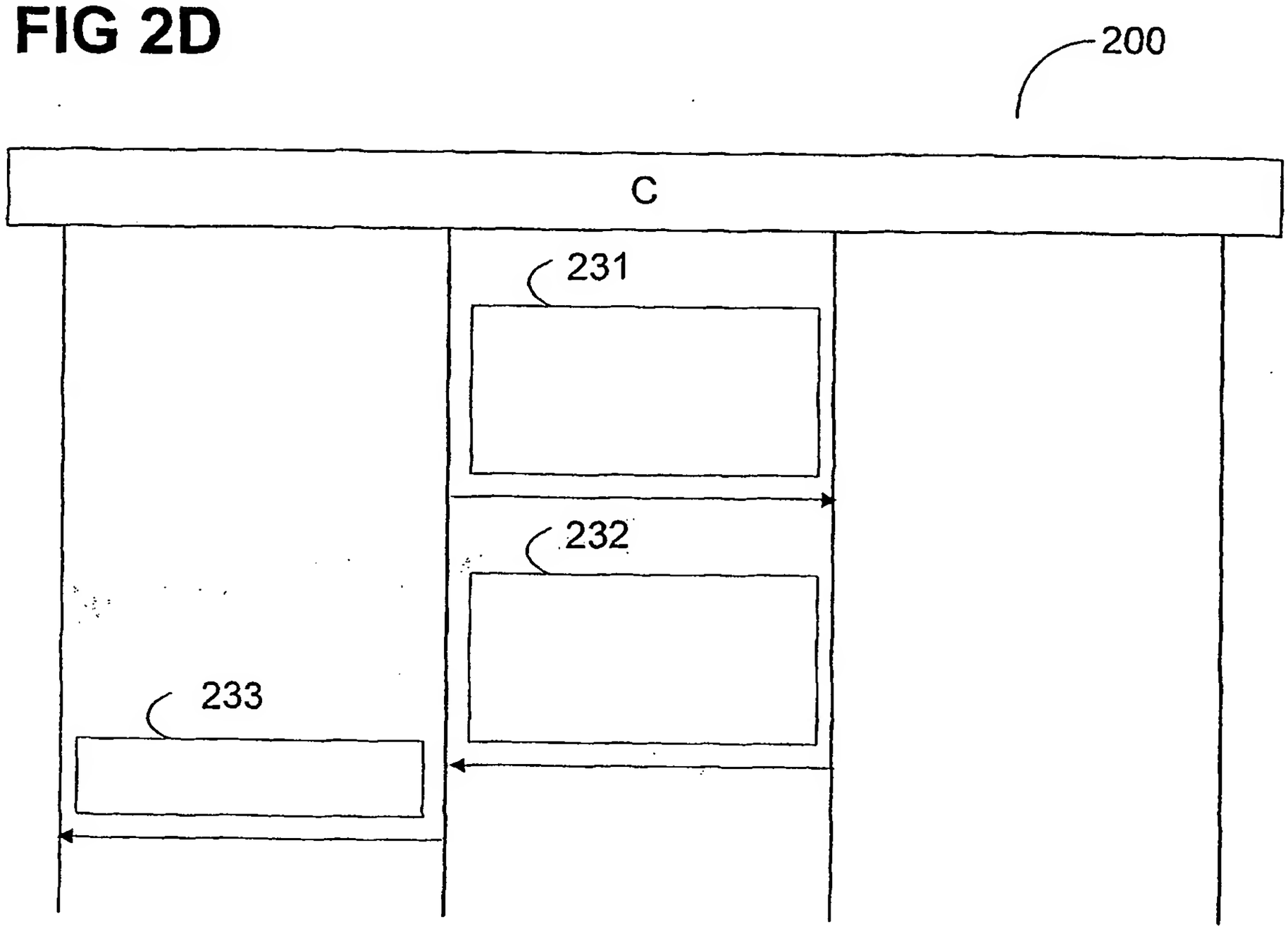


FIG 3A

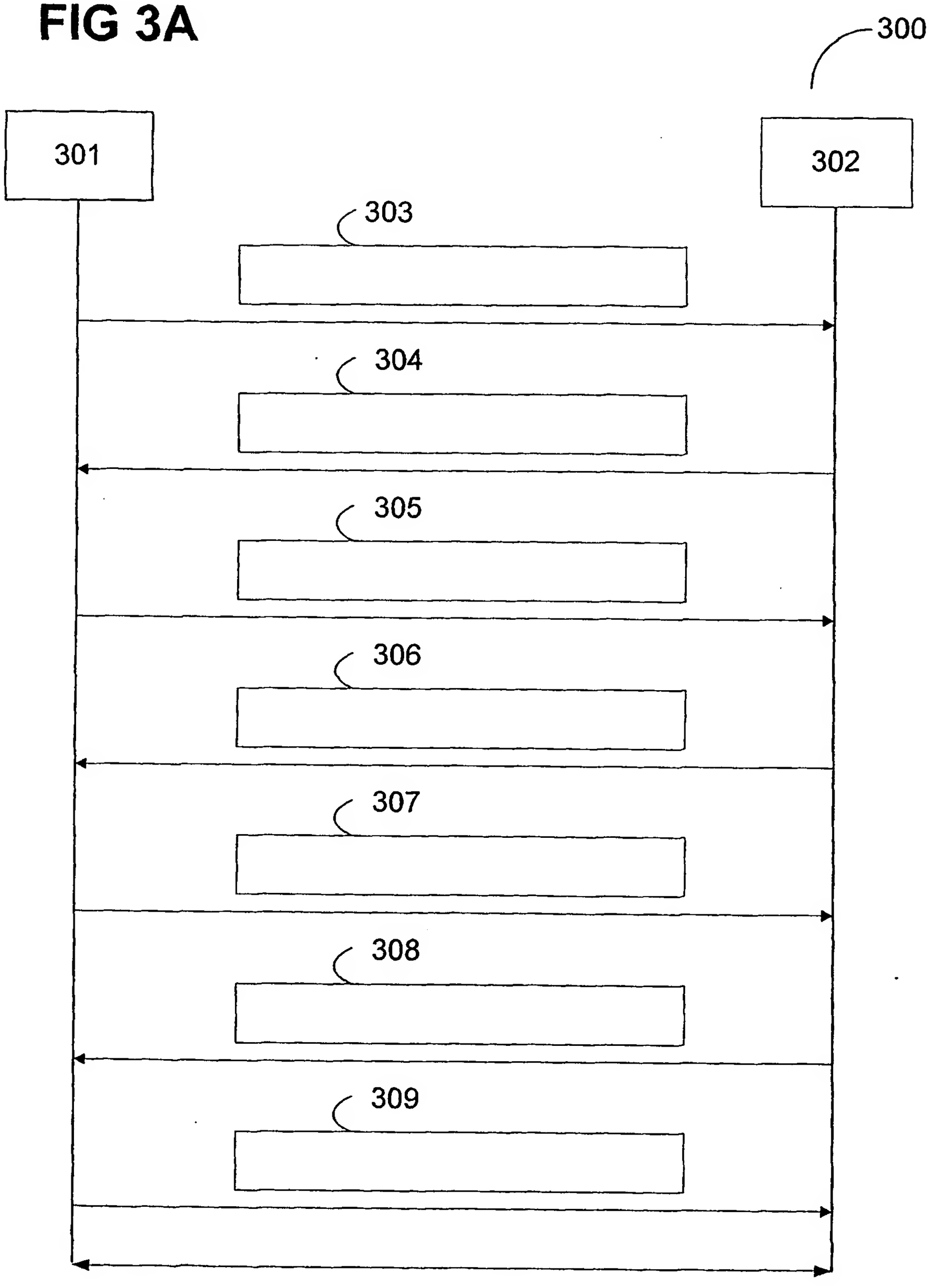
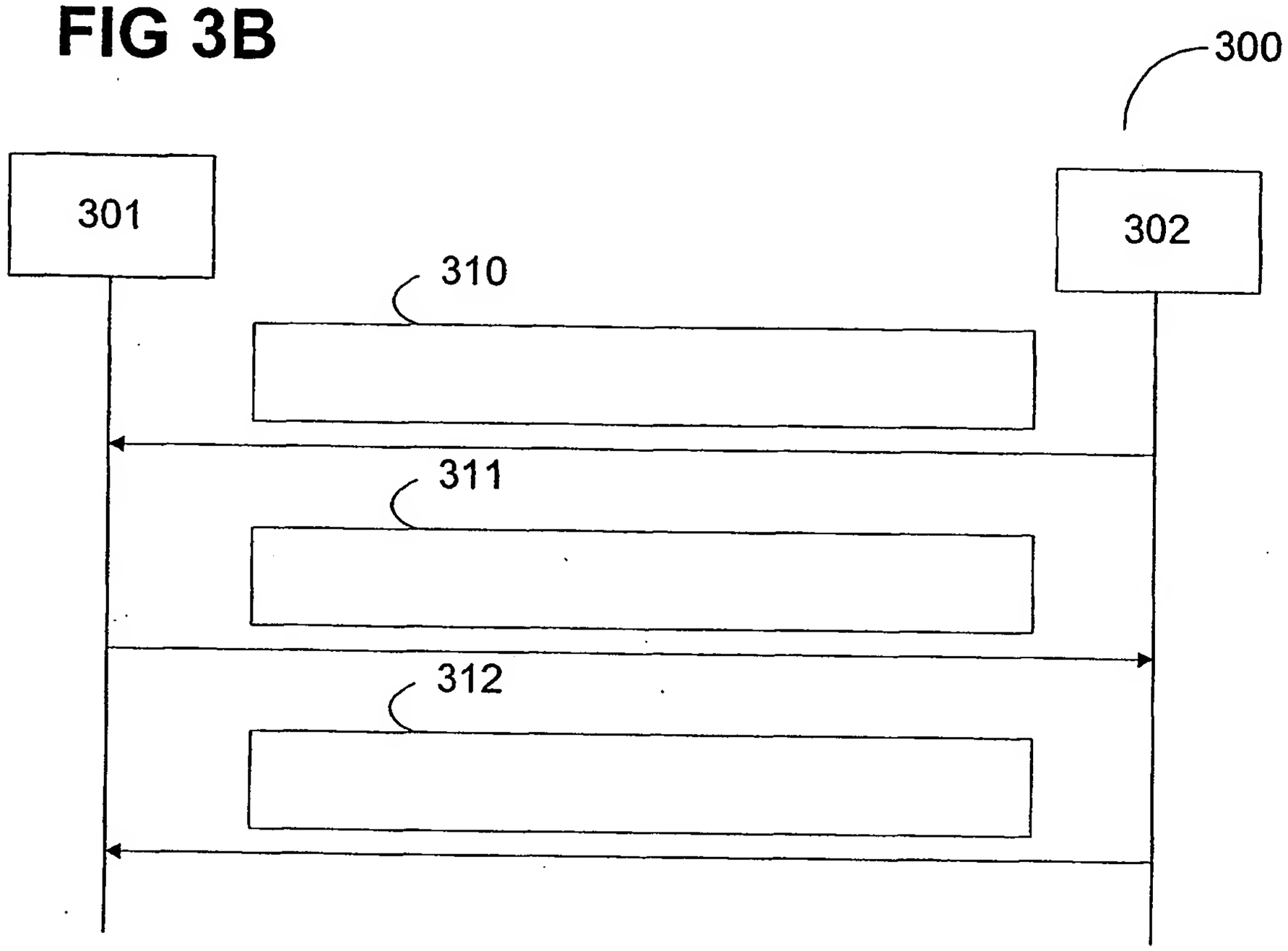


FIG 3B



# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051153

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/12 H04L12/28 H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | KAUFMAN C:<br>"draft-ietf-ipsec-ikev2-08.txt: Internet Key Exchange (IKEv2) Protocol"<br>INTERNET-DRAFT IPSEC WORKING GROUP,<br>May 2003 (2003-05), pages 1-97,<br>XP015002237<br>cited in the application<br>paragraph '001.! - paragraph '2.7.!;<br>figure 3<br>paragraph '3.14.! - paragraph '004.!<br>-/— | 1-14 |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" eartier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 13 October 2004 | 19/10/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Günther, S |

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051153

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | S. CHOKHANI, W. FORD, R. SABETT, C. MERRILL, S. WU: "draft-ietf-pkix-ipki-new-rfc2527-02.txt: Certificate Policy and Certification Practices Framework, Internet X.509 Public Key Infrastructure" INTERNET DRAFT PKIX WORKING GROUP, 22 April 2003 (2003-04-22), pages 1-81, XP015002989 paragraph '4.3.! - paragraph '4.4.12.! | 1-14 |
| A | PAUL FUNK; FUNK SOFTWARE, INC.; SIMON BLAKE-WILSON; BASIC COMMERCE &;INDUSTRIES, INC: "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)" INTERNET-DRAFT PPPEXT WORKING GROUP, November 2002 (2002-11), pages 1-40, XP015003044 cited in the application paragraph '001.! - paragraph '007.! paragraph '10.2.! - paragraph '012.! paragraph '014.! | 1-14 |
| A | MOLVA R: "INTERNET SECURITY ARCHITECTURE" COMPUTER NETWORKS AND ISDN SYSTEMS, NORTH HOLLAND PUBLISHING. AMSTERDAM, NL, vol. 31, no. 8, 23 April 1999 (1999-04-23), pages 787-804, XP000700282 ISSN: 0169-7552 paragraph '001.! - paragraph '3.2.!; figures 1,7 | 1-14 |
| A | RADIA PERLMAN: "draft-ietf-ipsec-ikev2-tutorial-01.txt: Understanding IKEv2: Tutorial, and rationale for decisions" IPSEC WORKING GROUP INTERNET-DRAFT, February 2003 (2003-02), pages 1-15, XP015002245 the whole document | 1-14 |
| A | T. KIVINEN: "draft-ietf-ipsec-dhcp-over-ike-00.txt: DHCP over IKE" INTERNET DRAFT IP SECURITY PROTOCOL WORKING GROUP IPSEC, 2 April 2003 (2003-04-02), pages 1-13, XP015002215 cited in the application paragraph '001.! - paragraph '004.! | 1-14 |

-/--

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/051153

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | D. FORSBERG; NOKIA; Y. OHBA; TOSHIBA; B. PATIL; NOKIA; H. TSCHOFENIG; SIEMENS; A. YEGIN; DOCOMO USA LABS: "draft-ietf-pana-pana-00.txt: Protocol for Carrying Authentication for Network Access (PANA)" INTERNET DRAFT, March 2003 (2003-03), pages 1-35, XP015002956 cited in the application paragraph '001.! paragraph '005.! | 1-14 |
| A | US 5 790 548 A (SISTANIZADEH KAMRAN ET AL) 4 August 1998 (1998-08-04) column 9, line 45 - column 14, line 32; figures 5,9 | 1-14 |

# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/EP2004/051153

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 5790548 A | 04-08-1998 | US 6452925 B1 | 17-09-2002 |
| | | US 6101182 A | 08-08-2000 |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/051153

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**
IPK 7 H04L29/06 H04L29/12 H04L12/28 H04L12/56

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

| Kategorie° | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | KAUFMAN C:<br>"draft-ietf-ipsec-ikev2-08.txt: Internet Key Exchange (IKEv2) Protocol"<br>INTERNET-DRAFT IPSEC WORKING GROUP,<br>Mai 2003 (2003-05), Seiten 1-97,<br>XP015002237<br>in der Anmeldung erwähnt<br>Absatz '001.! - Absatz '2.7.!; Abbildung 3<br>Absatz '3.14.! - Absatz '004.!<br>———<br>-/-- | 1-14 |

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 13. Oktober 2004 | 19/10/2004 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Günther, S |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/051153

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie° | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| A | S. CHOKHANI, W. FORD, R. SABETT, C. MERRILL, S. WU: "draft-ietf-pkix-ipki-new-rfc2527-02.txt: Certificate Policy and Certification Practices Framework, Internet X.509 Public Key Infrastructure" INTERNET DRAFT PKIX WORKING GROUP, 22. April 2003 (2003-04-22), Seiten 1-81, XP015002989 Absatz '4.3.! - Absatz '4.4.12.! | 1-14 |
| A | PAUL FUNK; FUNK SOFTWARE, INC.; SIMON BLAKE-WILSON; BASIC COMMERCE &;INDUSTRIES, INC: "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)" INTERNET-DRAFT PPPEXT WORKING GROUP, November 2002 (2002-11), Seiten 1-40, XP015003044 in der Anmeldung erwähnt Absatz '001.! - Absatz '007.! Absatz '10.2.! - Absatz '012.! Absatz '014.! | 1-14 |
| A | MOLVA R: "INTERNET SECURITY ARCHITECTURE" COMPUTER NETWORKS AND ISDN SYSTEMS, NORTH HOLLAND PUBLISHING. AMSTERDAM, NL, Bd. 31, Nr. 8, 23. April 1999 (1999-04-23), Seiten 787-804, XP000700282 ISSN: 0169-7552 Absatz '001.! - Absatz '3.2.!; Abbildungen 1,7 | 1-14 |
| A | RADIA PERLMAN: "draft-ietf-ipsec-ikev2-tutorial-01.txt: Understanding IKEv2: Tutorial, and rationale for decisions" IPSEC WORKING GROUP INTERNET-DRAFT, Februar 2003 (2003-02), Seiten 1-15, XP015002245 das ganze Dokument | 1-14 |
| A | T. KIVINEN: "draft-ietf-ipsec-dhcp-over-ike-00.txt: DHCP over IKE" INTERNET DRAFT IP SECURITY PROTOCOL WORKING GROUP IPSEC, 2. April 2003 (2003-04-02), Seiten 1-13, XP015002215 in der Anmeldung erwähnt Absatz '001.! - Absatz '004.! | 1-14 |

-/--

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/051153

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie° | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| A | D. FORSBERG; NOKIA; Y. OHBA; TOSHIBA; B. PATIL; NOKIA; H. TSCHOFENIG; SIEMENS; A. YEGIN; DOCOMO USA LABS: "draft-ietf-pana-pana-00.txt: Protocol for Carrying Authentication for Network Access (PANA)" INTERNET DRAFT, März 2003 (2003-03), Seiten 1-35, XP015002956 in der Anmeldung erwähnt Absatz '001.! Absatz '005.! | 1-14 |
| A | US 5 790 548 A (SISTANIZADEH KAMRAN ET AL) 4. August 1998 (1998-08-04) Spalte 9, Zeile 45 - Spalte 14, Zeile 32; Abbildungen 5,9 | 1-14 |

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2004/051153

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| US 5790548 A | 04-08-1998 | US 6452925 B1 | 17-09-2002 |
| | | US 6101182 A | 08-08-2000 |